1The opinion in support of the decision being entered today is *not* binding precedent of the Board.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte J. LESLIE VOGEL III

Appeal 2007-1121
Application 09/659,864
Technology Center 2100

Decided: October 19, 2007

Before KENNETH W. HAIRSTON, JEAN R. HOMERE, and JOHN A. JEFFERY, *Administrative Patent Judges*.

HOMERE, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

Appellant appeals under 35 U.S.C. § 134 from the Examiner's Final Rejection of claims 1 through 51. We have jurisdiction under 35 U.S.C. § 6(b) to decide this appeal. We affirm.

The Invention

Appellant invented a method and system for establishing a secure wireless communications channel encrypted with a channel key between an access point and a user station (Specification 4).

An understanding of the invention can be derived from exemplary independent claim 1, which reads as follows:

1. A computerized method of establishing a secure wireless communications channel between an access point and a station, the channel being encrypted with a channel key, the method comprising:

sending, by the station to the access point through a setup connection, a request for a security preference for the access point;

sending, by the access point to the station through the setup connection, the security preference in response to the request when the access point can support the channel, wherein the security preference specifies one authentication protocol from a set of authentication protocols supported by the access point;

generating, by the station, authentication information using a first key when the security preference is shared key;

sending, by the station to the access point through the setup connection, the authentication information;

validating, by the access point, the station using the authentication information; encrypting, by the access point, the channel key using a second key;

sending, by the access point to the station through the setup connection, the encrypted channel key;

decrypting, by the station, the channel key in response to receiving the encrypted channel key; and

sending, by the station to the access point, data encrypted with the channel key to establish the channel.

In rejecting the claims on appeal, the Examiner relies upon the following prior art:

Quick, Jr.	US 6,178,506 B1	Jan. 23, 2001 Filed Oct 23, 1998
Lewis	US 6,526,506 B1	Feb. 25, 2003 Filed Feb. 25, 1999

Schneier, B., "Applied Cryptography, Second Edition: Protocols,

Algorithms, and Source Code in C", 1996 pages 513-515.

ANSI/IEEE Std. 802.11, "Information technology-Telecommunication and information exchange between systems-Local and metropolitan area networks-specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications." 1999.

The Examiner rejects the claims on appeal as follows:

A. Claims 1 through 3, 9 through 17, 19 through 22, 24 through 27, 29 through 32, 34 through 38, 40 through 48, 50, and 51 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Lewis and Quick.

B. Claims 4 through 8, 18, 23, 28, 33, 39, and 49 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Lewis, Quick, and Schnieier.

First, Appellant contends[1] that the combined teachings of the references do render claims 1 through 51 unpatentable. Particularly, Appellant contends that neither Lewis nor Quick teaches or suggests an

[1] This decision considers only those arguments that Appellant submitted in the Appeal Brief of July 21, 2007 and the Reply Brief of January 12, 2007. Any other arguments that Appellant could have made but did not make in the Briefs are deemed to have been waived. *See* 37 C.F.R. § 41.37(c)(1)(vii)(eff. Sept. 13, 2004). *See also In re_Watts*, 354 F.3d 1362, 1368, 69 USPQ2d 1453, 1458 (Fed. Cir. 2004).

access point that supports a plurality of protocols, as recited in independent claim 1. (Br.6, Reply Br. 2). In response, the Examiner contends that Lewis' disclosure of a wireless network in accordance with the IEEE 802.11 standard teaches the cited limitation. (Answer 14).

Second, Appellant contends that the combination of Lewis and Quick does not teach or suggest generating authentication information using a key. (Br. 6, Reply 2). In response, the Examiner contends that Quick's disclosure of encrypting conventional registration information (ID and password) with a concatenated key teaches the cited limitation. (Answer 16).

ISSUE

The *pivotal* issue in the appeal before us is as follows:

Has Appellant shown[2] that the Examiner failed to establish that the combined disclosures of Lewis and Quick render the claimed invention

[2] In the examination of a patent application, the Examiner bears the initial burden of showing a prima facie case of unpatentability. *In re Piasecki,* 745 F.2d 1468, 1472, 223 USPQ 785, 788 (Fed. Cir. 1984). When that burden is met, the burden then shifts to the applicant to rebut. *Id.*; *see also In re Harris*, 409 F.3d 1339, 1343-44, 74 USPQ2d 1951, 1954-55 (Fed. Cir. 2005) (finding rebuttal evidence unpersuasive). If the applicant produces rebuttal evidence of adequate weight, the prima facie case of unpatentability is dissipated. *Piasecki*, 745 F.2d at 1472, 223 USPQ at 788. Thereafter, patentability is determined in view of the entire record. *Id.* However, Appellants have the burden on appeal to the Board to demonstrate error in the Examiner's position. *See In re Kahn*, 441 F.3d 977, 985-86, 78 USPQ2d 1329, 1335 (Fed. Cir. 2006) ("On appeal to the Board, an applicant can overcome a rejection [under § 103] by showing insufficient evidence of *prima facie* obviousness or by rebutting the *prima facie* case with evidence of secondary indicia of nonobviousness.") (quoting *In re Rouffet*, 149 F.3d 1350, 1355, 47 USPQ2d 1453, 1455 (Fed. Cir. 1998)).

unpatentable under 35 U.S.C. § 103(a)? Particularly, does the combination of Lewis and Quick render the claimed invention unpatentable, given that the cited combination teaches (1) a wireless network conforming to the IEEE 802.11 standard and (2) encrypting conventional registration information (ID and password) with a concatenated key?

FINDINGS OF FACT

The following findings of fact are supported by a preponderance of the evidence.

The Invention

1. As depicted in Figure 2, Appellant invented a method, system, and computer-readable medium for establishing a secure wireless communications channel (223) encrypted with a channel key between an access point (203) and a user station (201) (Specification 10).

2. Upon receiving a request for a connection (207) from the user station (201) through a setup connection (205), the access point (203) sends a security preference (209) to the user station (201) through the setup connection when the access point can support the channel. (*Id.* 11).

3. The security preference is a shared key that specifies an authentication protocol from a set of protocols supported by the access point.[3] (*Id.*).

[3] Particularly, at page 11, lines 4 through 7, Appellant's Specification states the following:

> The user station 201 sends a request 207 for a connection to the AP

4. Upon receiving the shared key, the user station uses a first key to generate authentication information, which is sent to the access point to validate the user station. After validating the user station, the access point uses a second key to encrypt the channel key, which is forwarded to the user station. The user station decrypts the channel key and returns the channel key to the access point with encrypted data to establish the communication channel between them. (*Id.* 11-12).

5. Appellant's background of the invention states the following:

> One approach to the problem of wireless connection security is addressed by the IEEE in the 802.11 standard for *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, Draft International Standard ISO/IEC 8802-11 IEEE P802.11/D10, 14 January 1999 (hereinafter "the 802.11 standard"). The 802.11 standard specifies an Infrastructure Network that provides wireless stations access to resources on a wired local area network (LAN) by way of an access point, such as a server on the wired LAN. *The Infrastructure Network can be secured using a shared key to establish a Wired Equivalency Privacy (WEP) connection between the access point and each station*, such as a desktop, laptop, or handheld computer. *The shared keys are distributed to the stations through secure channels outside the wireless network.*
> (Specification 3, emphasis added).

6. Appellant's Specification further states the following:

> The invention is particularly suited for use with Infrastructure

---

203. If the AP 203 can handle a new connection, it sends its security preference 209, in this case "shared key" to the user station 201. The request 207 and the security preferences 209 form an inquiry sequence 205 between the station 201 and the AP 203.

Networks defined by the 802.11 standard. An Infrastructure Network provides wireless stations access to resources on a wired LAN by way of an AP. *The AP specifies whether access to the LAN is open to all stations ("Open Systems") or secured through a Wired Equivalent Privacy (WEP) protocol using a shared key and a WEP encryption algorithm ("Shared Key").* The 802.11 standard assumes that the shared WEP key is distributed through some secure channel as described above by exchanging messages between the station and the AP using the 802.11 standard message format.
(Specification 19:1-9, emphasis added).

7. In the Appeal Brief, Appellant states the following:

Appellant respectfully submits that "open system" and "shared key" are well-known authentication protocols in the wireless networking art. In support of Appellant's assertion, Appellant is submitting , in the attached Evidence Appendix, *the section 8.1f IEEE 802.11 standard, which states that both "open system" and "shared key" are authentication services and further specifies the particular message frames that form the protocols for the two authentication services*.
(Brief 4, emphasis added).

The Prior Art Relied Upon

8. As depicted in Figure 1, Lewis teaches a multi-level encryption system for establishing a wireless communication channel between a mobile terminal (66) and an access point (54). (Col. 2, ll. 47-49; col. 4, ll. 28-34).

9. Lewis teaches a key distribution server (76) for providing access of an encryption key (authentication protocol) to an authorized mobile

terminal in response to a request from the mobile terminal to access the wireless network. The key distribution server subsequently informs the access point that the mobile station is authorized to access the system. (Col. 5, ll. 36-50).

10. The access point validates messages received from the mobile terminal by ensuring that the messages have been properly encrypted with the encryption key. (Col. 5, ll. 54-56).

11. Lewis teaches two types of encryption keys used in the disclosed system. First, the ENCRYPT key is used to encrypt and decrypt messages transmitted between the access point and the mobile terminal, and is similar to the encryption key used in the WEP protocol in the IEEE 802.11 standard. (Col. 6, ll. 43-51). Second, the MASTER key is programmed within the mobile terminal to encrypt messages transmitted from the mobile terminal to the key distribution server. (Col. 6, ll. 60-67).

12. The access point can provide the mobile terminal with a new ENCRYPT key using the previous encrypt key and instruct the processor in the mobile terminal to begin to use the new ENCRYPT key. (Col. 6, ll. 55-58).

13. Quick teaches a system for transferring the subscription of a wireless service to a new wireless terminal. Particularly, to register a new terminal to an existing wireless service, the subscriber enters personal

identification number and password. The terminal generates a public/private key pair, concatenates the public key with a random number and encrypts the concatenated number with a password. (Col. 4, ll. 45-58).

PRINCIPLES OF LAW

OBVIOUSNESS (Prima Facie)

The Supreme Court in *Graham v. John Deere Co.*, 383 U.S. 1, 17-18, 148 USPQ 459, 467 (1966), stated that the following factual inquiries underpin any determination of obviousness:

> Under § 103, [1] the scope and content of the prior art are to be determined; [2] differences between the prior art and the claims at issue are to be ascertained; and [3] the level of ordinary skill in the pertinent art resolved. Against this background, the obviousness or nonobviousness of the subject matter is determined. Such (4) secondary considerations as commercial success, long felt but unsolved needs, failure of others, etc., might be utilized to give light to the circumstances surrounding the origin of the subject matter sought to be patented. As indicia of obviousness or nonobviousness, these inquiries may have relevancy.

Where the claimed subject matter involves more than the simple substitution one known element for another or the mere application of a known technique to a piece of prior art ready for the improvement, a holding of obviousness must be based on "an apparent reason to combine the known elements in the fashion claimed." *KSR Int'l v. Teleflex, Inc.*, 127 S. Ct. 1727, 1740-41, 82 USPQ2d 1385, 1396 (2007). That is, "there must be

some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *Id.*, 127 S. Ct. at 1741, 82 USPQ2d at 1396 (quoting *In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006)). Such reasoning can be based on interrelated teachings of multiple patents, the effects of demands known to the design community or present in the marketplace, and the background knowledge possessed by a person having ordinary skill in the art. *KSR*, 127 S. Ct. at 1740-41, 82 USPQ2d at 1396.

ANALYSIS

35 U.S.C. § 103(a) REJECTION

We begin our analysis by first noting that, as set forth above, independent claim 1 requires that the access point send to the user station a security preference that specifies an authentication protocol from a set of authentication protocols supported by the access point. We find that the combination of Lewis and Quick reasonably teaches that limitation. As detailed in the Findings of Fact section above, we have found that Lewis teaches the access point for sending a new ENCRYPT key to the mobile terminal, where the new ENCRYPT key is intended to replace an existing ENCRYPT key that the key distribution server had used to transfer messages between the mobile terminal and the access point in response to a request made by the mobile terminal to access the wireless network. (Findings 8-10 and 12). Further, we have found that the ENCRYPT key is similar to the encryption key used in the WEP protocol in the IEEE 802.11

standard. (Finding 12). Additionally, we have found that under the IEEE 802.11 standard, "open system" and "shared key" are authentication protocols that are routinely used in the communication between an access point and a user station. (Finding 7). We agree with the Examiner that one of ordinary skill would have readily recognized that the disclosed ENCRYPT key conforming to the IEEE 802.11 standard teaches a security preference or authentication protocol (WEP) from the plurality of protocols routinely offered by the IEEE 802.11 standard. Similarly, the ordinarily skilled artisan would have recognized that the access point used in the IEEE 802.11 standard necessarily supports the plurality of protocols offered by that standard.[4] Therefore, we find no merit in Appellant's argument that Lewis' disclosure of exchanging network encryption keys does not teach the claimed exchange of security preferences. Similarly, we disagree with Appellant's argument that Lewis' disclosure of the new ENCRYPT key is not in response to a request submitted by the mobile terminal.

Second, as set forth above, we note that independent claim 1 further requires that the user station generate authentication information using a first key. We find that the combination of Lewis and Quick reasonably teaches

[4] We note that the limitation whereby the access point can support a plurality of protocols (as recited in claim 1) is inferred from the statement on page 11 of Appellant's Specification that *the request (207) and security preferences* ***(209)*** *form an inquiry sequence (205) between the user station (201) and the access point (203)*. Similarly, the WEP protocol in Lewis that conforms to the IEEE 802.11 standard, which entails a plurality of protocols in the communication of an access point and a user terminal, must necessarily involve a plurality of protocols supported by the access point.

that limitation. We have found in the Findings of Fact section above, that Quick teaches a terminal that concatenates a generated public key with a random number to encrypt conventional registration information (e.g. password) entered by a user. (Finding 13). We agree with the Examiner that one of ordinary skill in the art would have readily recognized that by encrypting the user-entered registration information with a generated key, the Quick's terminal generates authentication data permitting the new terminal to be registered for an existing wireless service. We affirm this rejection.

It follows that the Examiner did not err in rejecting independent claim 1 as being unpatentable over the combination of Lewis and Quick. We find

for these same reasons that claims 2, 3, 9 through 17, 19 through 22, 24 through 27, 29 through 32, 34 through 38, 40 through 48, 50, and 51 are unpatentable over the combination of Lewis and Quick. We affirm this rejection.

Now, we turn to the rejection of claims 4 through 8, 18, 23, 28, 33, 39 and 49 as being unpatentable over the combination of Lewis, Quick, and Schnieier. Appellant reiterates that the combination of Lewis and Quick fails to teach or suggest an access point that sends a security preference to a user terminal. We have already addressed this argument in the discussion of independent claim 1 above, and we disagreed with Appellant. Appellant further contends that Schnieier does not cure the alleged deficiencies of the Lewis and Quick combination. We find no such deficiencies in the cited combination for Schnieier to cure. It follows that the Examiner did not err in rejecting claims 4 through 8, 18, 23, 28, 33, 39, and 49 as being unpatentable over the combination of Lewis, Quick, and Schnieier. We affirm this rejection.

CONCLUSION OF LAW

On the record before us, Appellant has not shown that the Examiner failed to establish that claims 1 through 3, 9 through 17, 19 through 22, 24 through 27, 29 through 32, 34 through 38, 40 through 48, 50, and 51 are unpatentable over the combination of Lewis and Quick under 35 U.S.C. § 103. Similarly, Appellant has not shown that the Examiner failed to establish that claims 4 through 8, 18, 23, 28, 33, 39, and 49 are unpatentable over the combination of over Lewis, Quick, and Schnieier under 35 U.S.C. § 103.

DECISION

We have affirmed the Examiner's decision rejecting claims 1 through 51.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

eld

Sheryl Sue Holloway
Blakely Sokoloff Taylor & Zafman LLP
12400 Wilshire Boulevard 7th Floor
Los Angeles CA 90025